



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/617,215	07/07/2003	Francesco Grilli	030337	3124

23696 7590 03/13/2009  
QUALCOMM INCORPORATED  
5775 MOREHOUSE DR.  
SAN DIEGO, CA 92121

EXAMINER
----------

DADA, BEEMNET W

ART UNIT	PAPER NUMBER
----------	--------------

2435

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

03/13/2009

ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com  
kascanla@qualcomm.com  
nanm@qualcomm.com

<b>Office Action Summary</b>	<b>Application No.</b> 10/617,215	<b>Applicant(s)</b> GRILLI ET AL.	
	<b>Examiner</b> BEEMNET W. DADA	<b>Art Unit</b> 2435	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 02 December 2008.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-61 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-3, 5, 8-14, 18-24, 26, 29-33, 37-43, 45, 48-54 and 58-61 is/are rejected.
- 7) ☒ Claim(s) 4, 6, 7, 15-17, 25, 27, 28, 34-36, 44, 46, 47 and 55-57 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                     | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

## **DETAILED ACTION**

This office action is in reply to an amendment filed on December 02, 2008. Claim 22 has been amended. Claims 1-61 are pending.

### ***Response to Arguments***

Applicant's arguments with respect to 35 USC 101 rejections of claims 22-40 have been fully considered and are persuasive. The rejection has been withdrawn.

Applicant's arguments with respect to 35 USC 103(a) rejections of claims 1, 22, 41, 12, 31 and 52 have been fully considered but they are not persuasive.

Applicant argues that Faccin (US 6,879,690 B2) does not disclose generating a radio access key (RAK) as a function of a random number and a key selected from a group consisting of a public land mobile key (PK) and a broadcast access key (BAK). Applicant further argues that, instead, the long term key of Faccin is similar to the permanent user specific registration key (RK) discussed in paragraph 1016 of the present application. Examiner disagrees.

Examiner would point out that Faccin teaches generating a radio access network key (RAK) (i.e., generating new TSK value) as a function of the random number (i.e., RANDTSK) and a key selected from the group consisting of a public land mobile network key (PK) and a broadcast access key (BAK) (i.e., long-term key) [column 10, lines 45-47 and figure 5]. Note that, the radio access network key (RAK) is generated using a random number and either PK or BAK. Both PK and BAK are encryption/decryption and/or authentication keys, which are equivalent to the long-term key taught by Faccin.

Applicant argues that Shibata (US 2004/0019787 A1) teaches a user manually inputting certain information such as a user ID, password or received account information, and applicant pointed out that this is not the same field of endeavor as Faccin and if combined would modify Faccin to require manual entry of a user ID or password to identify the person using the mobile node. Applicant further argue that, 'User identification number' is described as a P-TMSI, IMSI, electronic serial number (ESN) ..." in the present application. This is different than the manually input user ID or password described in Shibata. Examiner disagrees.

Examiner would point out that, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., User identification number is described as a P-TMSI, IMSI, electronic serial number (ESN)) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Examiner would further point out that, the claimed invention does not limit the user identification information from being manually entered. Examiner would further point out that, Both Faccin and Shibata are directed to authentication of communication terminals and therefore, are directed to the same field of endeavor.

Applicant further argues that, Faccin fails to teach receiving a provisioning message from a broadcast-multicast service center and/or wherein the PK is extracted from a provisioning message received from a broadcast multicast service center. Examiner disagrees.

Examiner would point out that, Faccin teaches receiving a provisioning message from a broadcast-multicast service center and/or wherein the PK is extracted from a provisioning message received from a broadcast multicast service center [column 8, lines 29-51, figure 4 and 5].

Applicant's arguments with respect to claims 4, 6, 7, 15, -17, 25, 27, 28, 34-36, 44-47, 55-57 have been considered and are persuasive and therefore the rejections of these claims has been withdrawn.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-3, 5, 8-14, 18-24, 26, 29-33, 37-43, 45, 48-54 and 58-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Faccin et al. US 6,879,690 B2 (hereinafter Faccin) in view of Shibata US 2004/0019787 A1.

As per claims 1, 22 and 41, Faccin teaches a method of obtaining secure registration by a memory module (UICC) in a multicast-broadcast-multimedia system (MBMS), the method comprising:

receiving a random number (RANDTSK, column 9, lines 63-67 and column 10, lines 11-14);

generating a radio access network key (RAK) (i.e., generating new TSK value) as a function of the random number (i.e., RANDTSK) and a key selected from the group consisting of a public land mobile network key (PK) and a broadcast access key (BAK) (i.e., long-term key) [column 10, lines 45-47 and figure 5];

generating a temporary registration key (RGK) (i.e., AUTHU) as a function of the RAK [column 10, lines 63 -67], and

authenticating at least one registration message in the MBMS based on the RGK  
[column 10, line 64-67 and column 8, lines 29-47]

Faccin as indicated above teaches generating a temporary registration key (RGK) as a function of the RAK (access network key). Faccin is silent on generating temporary registration key (RGK) as a function of the RAK (access network key) and a user identification number. However, in the same field of endeavor, Shibata teaches generating a temporary key (session key) as a function of an RAK (i.e., access key) and a user identification number (i.e., user ID) [see paragraphs 0062 and 0081-0083]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Shibata within the system of Faccin in order to enhance the security of the system.

As per claims 12, 31 and 52, Faccin teaches a method of obtaining secure registration by a mobile station in a multicast-broadcast-multimedia system (MBMS), the method comprising:

receiving a random number from a radio access network (i.e., AAAv receiving RANDTSK, column 10, lines 11-13);

transmitting the random number to a memory module (UICC) (i.e., transmitting RANDTSK to mobile node/device, column 10, lines 11-14);

receiving from the UICC a temporary registration key (RGK) based on the random number [column 10, lines 45-60], and

authentication at least one registration message in the MBMS based on the RGK  
[column 10, line 64-67 and column 8, lines 29-47].

Faccin as indicated above teaches receiving a temporary registration key (RGK) based on a random number. Faccin is silent on receiving a temporary registration key (RGK) based on

Art Unit: 2435

the random number and a user identification number. However, in the same field of endeavor, Shibata teaches receiving a temporary key (session key) as a function of an RAK (i.e., access key) and a user identification number (i.e., user ID) [see paragraphs 0062 and 0081-0083]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Shibata within the system of Faccin in order to enhance the security of the system.

As per claims 2, 23 and 42, Faccin further teaches the method further comprising transmitting the RGK to a mobile telephone [column 10, lines 60-67].

As per claims 3, 4, 24, 26, 43 and 45, Faccin further teaches the method further comprising receiving a provisioning message from a broadcast-multicast service center [figure 4 and 5].

As per claims 8, 18, 37, 48 and 58, Faccin further teaches the method wherein the UICC comprises a subscriber identity module (SIM) in a GSM system [figures 1 and 2].

As per claims 9, 19, 38, 49 and 59, Faccin further teaches the method wherein the UICC comprises a RUIM in CDMA system [figures 1 and 2].

As per claims 10, 11, 20, 21, 29, 30, 39, 40, 50, 51, 60 and 61, Faccin further teaches the method wherein the PK/BAK is provisioned by using a public key [column 10, lines 25-67].

As per claims 13, 32 and 53, Faccin further teaches the method wherein the RGK is a function of a radio access network key (RAK) which is a function of the random number and a key selected from the group consisting of a public land mobile network key (PK) and a broadcast access key (BAK) [column 10, lines 45-47 and figure 5].

As per claims 14, 33 and 54, Faccin further teaches the method wherein the PK is extracted from a provisioning message received from a broadcast-multicast service center [figure 4 and 5].

### ***Allowable Subject Matter***

Claims 4, 6, 7, 15-17, 25, 27, 28, 34-36, 44-47 and 55-57 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.



Any inquiry concerning this communication or earlier communications from the examiner should be directed to BEEMNET W. DADA whose telephone number is (571)272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Beemnet W Dada/  
Examiner, Art Unit 2435  
March 10, 2009